Amendments to the Specification:

In the Abstract:

Please cancel the previous Abstract and substitute the Abstract on the accompanying separate sheet.

Page 2:

Please substitute the following paragraph for the paragraph beginning at line 22:

The method for verifying the source of the request to certify a public key ~~derived from~~ of a pair of asymmetric keys, a public key Kp and a private key Ks, generated for a given algorithm CA1 and a given usage, such as encryption/decryption or digital signature verification/generation, by an embedded system and stored in the storage area of an embedded system Si equipped with cryptographic calculation means and externally accessible read/write-protected means for storing digital data, this digital data IDd_i comprising at least a serial number SN_i for identifying the embedded system and an identification code OP_j of an operator authorized to configure said embedded system, this request being formulated by said embedded system by transmitting a request message MRCA containing said public key Kp to a certification authority CA, is remarkable in that it consists, prior to any transmission of a certification request, during the configuration of these embedded systems by this authorized operator, for all the embedded systems Si of a set Lk of embedded systems:

Page 4:

Please add the following paragraph before line 9:

Fig. 4c represents, by way of non-limiting example, the structure of the certification request template GRCA.

Page 13:

Please substitute the following paragraph for the paragraph beginning at line 9:

The key diversification process implemented in step 1003, as represented in Fig. 3, can thus consist in a process supported by an algorithm known as a Zero Knowledge Signature ~~Mechanism~~ Mechanisms and the algorithms ~~known by the names~~ such as the FIAT-SHAMIR or GUILLOU QUISQUATER algorithms that are usable for this purpose. For this reason, as indicated in Fig. 3, each diversified private key KsM_i is considered to have been obtained by implementing processes supported by the FIAT-SHAMIR algorithm F-S or the GUILLOU-QUISQUATER algorithm G-Q and thus verifies the relation:

Page 14:

Please substitute the following paragraph for the paragraph beginning at line 22:

Fig. 4b, at point 1), represents the structure of a certification request template GRCA in such a case, which is considered to be formed by a set of fields TLV that are sequential or interleaved in accordance with the ~~ASN1~~ ANS1 standard. This request template is formed outside the embedded system. It must include, and this is verified by the embedded system, three fields and three fields only, which correspond to: 1) a type of algorithm identifying field, 2) a type of public key value field, 3) a type of public key usage indicator field. The position of each of these fields among the other fields of the request template must also correspond to a precise position, i.e. it must be preceded and followed by predetermined different types of fields.